What is claimed is:

1. A method for backing up a biometrics-based authentication device comprising the steps of:

obtaining a first encryption key;

enciphering lower tier data with said first encryption key to generate an encrypted lower tier backup file;

obtaining a second encryption key; and

enciphering upper tier data with said second encryption key to generate an encrypted upper tier backup file, wherein said lower tier data contain encrypted identification of a user and authentication information associated therewith and wherein said upper tier data contain biometrics data of said user and said lower tier data encrypted with said first encryption key.

2. The method according to claim 1, wherein

said authentication information comprises private keys and corresponding certificates.

3. The method according to claim 1, further comprising the step of:

generating a restore validation script for establishing restore requirements of said upper tier data.

4. The method according to claim 3, wherein

said upper tier data further contain said restore validation script.

5. The method according to claim 1, further comprising the step of:

establishing a secure connection with a service bureau.

6. The method according to claim 5, further comprising the step of:

obtaining said first and said second encryption keys from said service bureau.

7. The method according to claim 1, further comprising the step of:

storing said encrypted lower tier backup file and said encrypted upper tier backup file as one or more physical files.

8. A method for restoring onto a new biometrics-based authentication device said lower tier data and said upper tier data according to claim 1, comprising the steps of:

enrolling new biometrics data of said user onto said new biometrics-based authentication device;

obtaining an upper tier data decryption key;

deciphering said encrypted upper tier backup file with said upper tier data decryption key to generate decrypted upper tier data including decrypted biometrics data;

determining, based on said decrypted biometrics data, whether said new biometrics data are valid;

obtaining a lower tier data decryption key when said new biometrics data are valid;

deciphering said encrypted lower tier data with said lower tier data decryption key to generate decrypted lower tier data; and

storing said decrypted lower tier data onto said new biometrics-based authentication device.

9. The method according to claim 8, further comprising the steps of:

uploading said encrypted lower tier backup file and said encrypted upper tier backup file onto said new biometrics-based authentication device;

obtaining an access clearance from a service bureau; and

establishing a secure connection with said service bureau using said access clearance.

10. The method according to claim 9, further comprising the step of:

obtaining said upper tier data decryption key and said lower tier data decryption key from said service bureau.

11. The method according to claim 8, further comprising the step of:

verifying that said decrypted upper tier data have not been tampered or altered.

12. An apparatus for implementing the method according to claim 1 or 8, wherein said apparatus is configured to perform the steps of claim 1 or 8.

13. An article of manufacture for implementing the method according to claim 1 or 8, wherein said article of manufacture comprising a computer readable medium carrying computer-executable instructions implementing the steps of claim 1 or 8.